Passively self-error-rejecting single-qubit transmission over a collective-noise channel

Fu-Guo Deng,[1] Xi-Han Li,[2] and Hong-Yu Zhou[2]
[1] *Department of Physics, Applied Optics Beijing Area Major Laboratory, Beijing Normal University, Beijing 100875, China*
[2] *Institute of Low Energy Nuclear Physics, and Department of Material Science and Engineering, Beijing Normal University, Beijing 100875, China*

(Dated: February 2, 2008)

We propose a passively self-error-rejecting single-qubit transmission scheme of an arbitrary polarization state of a single qubit over a collective-noise channel, without resorting to additional qubits and entanglements. By splitting a single qubit into some wavepackets with some Mach-Zehnder interferometers, we can obtain an uncorrupted state with a success probability approaching 100% via postselection in different time bins, independent of the parameters of collective noise. It is simpler and more flexible than the schemes utilizing decoherence-free subspace and those with additional qubits. One can directly apply this scheme to almost all quantum communication protocols against collective noise, including the decoy-state quantum key distribution protocols with faint laser pulses.

PACS numbers: 03.67.Pp, 03.67.Dd, 03.67.Hk

Quantum key distribution (QKD) supplies a secure way for two parties, say the sender Alice and the receiver Bob, to generate a private key, provided that they initially share a short secret key (for identity authentication) and that they possess an unprotected quantum channel (an optical fiber). Different from classical cryptosystem in which the secrecy of key depends on computation difficulty with a limited computation power, the security of QKD comes from the laws of quantum mechanics such as the uncertain relation (non-cloning theorem), the coherence of entangled systems, quantum measurement, and so on. As an unknown quantum state cannot be cloned, the vicious actions done by an eavesdropper, say Eve will inevitably disturb the quantum system and leave a trace in the outcomes obtained by the two authorized parties. Eve's action will be detected by analyzing the error rate of samples chosen randomly. Since Bennett and Brassard published the original QKD protocol [1] in 1984 (called BB84), QKD attracts a great deal of attention [2] and has been proven unconditionally secure [3, 4].

Implementations of practical QKD rely on either the polarization or the phase of photons. Preventing Eve from eavesdropping by disguising her action as noise with a better quantum channel requires the two legitimate users to control the influence of the noise in their quantum channels. Otherwise, they can only distil a short private key from a large raw string with privacy amplification [2]. When the noise in the quantum channels is too large, secure key generation is impossible. For overcoming the birefringence of the optical fiber which alters the polarization state of photons, some QKD schemes are proposed with Mach-Zehnder interferometers (MZIs) and a Faraday mirror which is used to compensate polarization mode dispersion, such as the "plug and play" QKD system [5] and its modification [6, 7]. However, these two-way quantum communication schemes are vulnerable to the Trojan horse attack [2]. Recently, some novel techniques are developed for protecting quantum information transmission, such as decoherence-free subspaces (DFS) [8, 9], error-correcting codes [10], faithful qubit distribution [11], faithful qubit transmission [12], error-rejecting codes [13], and so on. In DFS, a single logical qubit is encoded in two physical qubits [14], i.e., $|\bar{0}\rangle \rightarrow |HV\rangle$, $|\bar{1}\rangle \rightarrow |VH\rangle$. Here $|H\rangle$ and $|V\rangle$ represent the horizontal polarization and the vertical polarization, respectively. This code makes the logical qubits be immune to a collective-dephasing noise which is described with a transformation [9]: $|H\rangle \rightarrow |H\rangle$, $|V\rangle \rightarrow e^{i\phi}|V\rangle$ (the additional phase ϕ is unknown to any one). Under this transformation, the states of two physical qubits $|HV\rangle$, $|VH\rangle$, and $\frac{1}{\sqrt{2}}(|HV\rangle \pm |VH\rangle)$ all are immune to this collective-dephasing noise, and can be used for quantum communication perfectly [9]. Wang showed that DFS can also used for QKD over a collective- random-unitary-noise channel by checking parity and sacrificing a proportion of qubits [15] . In error-correcting codes [10], at least five entangled physical qubits are encoded for a single logical qubit against the noise. In 2005, Yamamoto et al. [11] introduced a good way for faithful qubit distribution with one additional qubit against collective noise. Their scheme can be perfectly used for secure key generation with two quantum channels. The proportion of uncorrupted qubits to those transmitted approaches 1/8. More recently, a scheme [12] for faithful qubit transmission without additional qubits is proposed with two quantum channels. Its proportion of uncorrupted qubits to those transmitted approaches 1/2 in a passive way. With some delayers, the proportion can be improved to 1. In the error-rejecting codes [13], at least two fast polarization modulators (Pockels cell), whose synchronization makes it difficult to be implemented with current technology [16], are employed [12].

Here we introduce a scheme for passively self-error-rejecting single-qubit transmission over a collective noise channel with a success probability approaching 100%, several times of other schemes. For example, the success probability in the present scheme is about eight times as that in the scheme proposed by Yamamoto et al.[11] in a passive way. Moreover, it is independent of the parameters of collective noise. Unlike other schemes [9, 15, 17, 18], it does not require entanglements. Different from Yamamoto's scheme [11], the present scheme needs no additional qubits. This feature makes the present scheme more flexible than the latter as there is not a practical single-photon source at present and it is difficult to obtain two single photons in a deterministic time. Our scheme works with one quantum channel, not two [11, 12] or more, and its implement is based on some simple optical devices. All these good features make it easy to apply for almost all quantum communication protocols existing, including the decoy-state QKD protocols [19, 20, 21] with faint laser pulses.

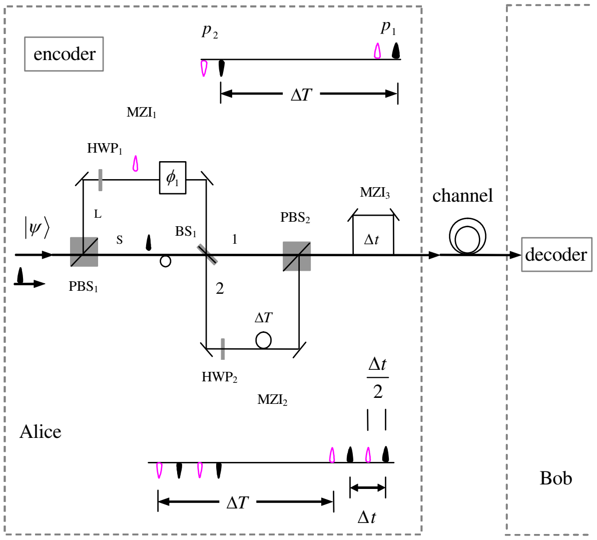

FIG. 1: Schematic representation of self-error-rejecting single-qubit transmission over a collective-noise channel. PBS$_i$ ($i = 1, 2$), HWP, and BS$_i$ represent polarizing beam splitter, half wave plate, and beam splitter (50/50), respectively. MZI$_i$ represent unbalanced Mach-Zehnder interferometers. The intervals between the long path and the short path in MZI$_1$, MZI$_2$, and MZI$_3$ are $\frac{\Delta t}{2}$, ΔT, and Δt, respectively. P_1 and P_2 represent the two output ports of the BS$_1$. $\phi_1 = \frac{3\pi}{2}$.

The principle of our self-error-rejecting single-qubit transmission scheme over a collective-noise channel is shown in Fig.1. It comprises an encoder, a collective-noise channel in which the fluctuation is slow in time so that the alteration of the polarization is considered to be the same over the sequence of several photons (or wavepackets) [11], and a decoder. The encoder is made up of three unbalanced Mach-Zehnder interferometers (MZI) with different intervals. A single qubit, whose original state is $|\psi\rangle = \alpha|H\rangle + \beta|V\rangle$, is split into two parts by the first polarizing beam splitter (PBS), which transmits $|H\rangle$ and reflects $|V\rangle$. A half wave plate (HWP) rotates the polarization of the photons in the path L by 90^o. A phase modulator compensates a relative pase $e^{i\phi_1}$ on the part passing through the path L. Before the first beam splitter (BS:50/50), the state of the single qubit can be described as $|\psi\rangle = \alpha|H\rangle_S + e^{i\phi_1}\beta|H\rangle_L$. Let us set $\phi_1 = \frac{3\pi}{2}$. The time of flight difference of MZI$_2$ is set to be ΔT which is far larger than that of MZI$_1$ ($\frac{\Delta t}{2} \equiv t_L - t_S$), shown at the top of the Fig.1. Therefore, the single qubit before it enters the collective-noise channel is in the state

$$\begin{aligned}|\psi\rangle_c &= \frac{1}{2}\{[\alpha(|H\rangle_0 + |H\rangle_{\Delta t}) + \beta(|H\rangle_{\frac{\Delta t}{2}} + |H\rangle_{\frac{3\Delta t}{2}})]_1 \\ &- i[\alpha(|V\rangle_0 + |V\rangle_{\Delta t}) + \beta(|V\rangle_{\frac{\Delta t}{2}} + |V\rangle_{\frac{3\Delta t}{2}})]_2\}, \quad (1)\end{aligned}$$

where the complex coefficient i comes from the phase shift aroused by the BS$_1$ reflection (we assume that the first surface of the BS$_1$ has the phase shift i and the second surface has $-i$), and the subscripts 1 and 2 represent the two output ports of the BS$_1$.

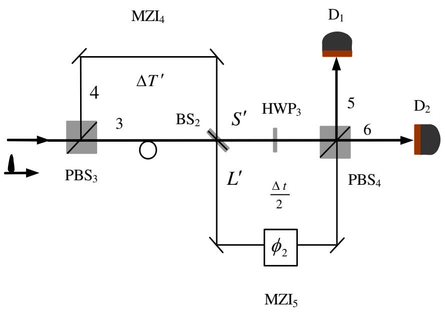

FIG. 2: A decoder for self-error-rejecting single-qubit transmission over a collective noise channel. The intervals between the long path and the short path in MZI$_4$ and MZI$_5$ are $\Delta T'$ and $\frac{\Delta t}{2}$, respectively. $\phi_2 = \frac{\pi}{2}$.

As the wavepackets passing through the port 1 and 2 have no overlap, the single qubit is split into eight wavepackets by the encoder, shown in the bottom of Fig.1. Suppose that each collective noise transforms the polarization states as

$$\begin{aligned}|H\rangle &\rightarrow \delta_1|H\rangle + \gamma_1|V\rangle, \\ |V\rangle &\rightarrow \delta_2|H\rangle + \gamma_2|V\rangle, \quad (2)\end{aligned}$$

where

$$|\delta_1|^2 + |\gamma_1|^2 = |\delta_2|^2 + |\gamma_2|^2 = 1. \quad (3)$$

These rotations transform the state (1) into

$$\begin{aligned}|\psi\rangle_d &= \frac{1}{2}\{\delta_1[\alpha(|H\rangle_0 + |H\rangle_{\Delta t}) + \beta(|H\rangle_{\frac{\Delta t}{2}} + |H\rangle_{\frac{3\Delta t}{2}})]_1 \\ &+ \gamma_1[\alpha(|V\rangle_0 + |V\rangle_{\Delta t}) + \beta(|V\rangle_{\frac{\Delta t}{2}} + |V\rangle_{\frac{3\Delta t}{2}})]_1 \\ &- i\delta_2[\alpha(|H\rangle_0 + |H\rangle_{\Delta t}) + \beta(|H\rangle_{\frac{\Delta t}{2}} + |H\rangle_{\frac{3\Delta t}{2}})]_2 \\ &- i\gamma_2[\alpha(|V\rangle_0 + |V\rangle_{\Delta t}) + \beta(|V\rangle_{\frac{\Delta t}{2}} + |V\rangle_{\frac{3\Delta t}{2}})]_2\}. \\ &\quad (4)\end{aligned}$$

A decoder for self-error-rejecting single-qubit transmission is shown in Fig.2. The PBS$_3$ is used to pick out the state $|V\rangle$ from the state $|H\rangle$ with a time delay $\Delta T'$. Thus, the four states $[\alpha(|H\rangle_0 + |H\rangle_{\Delta t}) + \beta(|H\rangle_{\frac{\Delta t}{2}} + |H\rangle_{\frac{3\Delta t}{2}})]$, $[\alpha(|V\rangle_0 + |V\rangle_{\Delta t}) + \beta(|V\rangle_{\frac{\Delta t}{2}} + |V\rangle_{\frac{3\Delta t}{2}})]_{\Delta T'}$, $[\alpha(|H\rangle_0 + |H\rangle_{\Delta t}) + \beta(|H\rangle_{\frac{\Delta t}{2}} + |H\rangle_{\frac{3\Delta t}{2}})]_{\Delta T}$, and $[\alpha(|V\rangle_0 + |V\rangle_{\Delta t}) + \beta(|V\rangle_{\frac{\Delta t}{2}} + |V\rangle_{\frac{3\Delta t}{2}})]_{\Delta T+\Delta T'}$ are distinguished with different time bins by the MZI$_2$ and MZI$_4$. We consider only the state $|\psi'\rangle \equiv \alpha(|H\rangle_0 + |H\rangle_{\Delta t}) + \beta(|H\rangle_{\frac{\Delta t}{2}} + |H\rangle_{\frac{3\Delta t}{2}})$ to be used for reconstructing the original state $|\psi\rangle = \alpha|H\rangle + \beta|V\rangle$ below. The other three states with delays ΔT, $\Delta T'$, and $\Delta T + \Delta T'$ can also be used for reconstructing the original state $|\psi\rangle$ in the same way with or without a unitary operation.

The BS$_2$ splits the state $|\psi'\rangle = \alpha(|H\rangle_0 + |H\rangle_{\Delta t}) + \beta(|H\rangle_{\frac{\Delta t}{2}} + |H\rangle_{\frac{3\Delta t}{2}})$, which passes through the output port 3 of the BS$_2$ without delay, into two parts and then they combine with each other at the PBS$_4$. The part through the long path (L') of the MZI$_5$ are compensated a phase shift $\phi_2 = \frac{\pi}{2}$ and the polarization state of the part through the short path (S') is rotated 90^o by the third half wave plate (HWP$_3$). Before the PBS$_4$, the state of the two parts becomes

$$\begin{aligned} |\psi'\rangle \xrightarrow{MZI_5} & \; |\psi''\rangle \\ = & \; \frac{1}{\sqrt{2}}\{\alpha(|V\rangle_0 + |V\rangle_{\Delta t}) + \beta(|V\rangle_{\frac{\Delta t}{2}} + |V\rangle_{\frac{3\Delta t}{2}}) \\ + & \; \alpha(|H\rangle_{\frac{\Delta t}{2}} + |H\rangle_{\frac{3\Delta t}{2}}) + \beta(|H\rangle_{\Delta t} + |H\rangle_{2\Delta t})\}. \end{aligned} \tag{5}$$

The receiver Bob can perfectly reconstruct the original state $|\psi\rangle = \alpha|H\rangle + \beta|V\rangle$ at the time bins $\frac{\Delta t}{2}$ and $\frac{3\Delta t}{2}$ without unitary operations when the single qubit emerges in port 5, which takes place with success probability 1/2. Also he can obtain the state $|\psi\rangle$ at the time bin Δt with a bit-flip operation $\sigma_x = |H\rangle\langle V| + |V\rangle\langle H|$ when the single qubit emerges in port 5, which takes place with success probability 1/4, shown in Fig.3. That is, Bob has the success probability $P_s = 3/4$ to obtain the uncorrupted state. In a word, with the encoder shown in Fig.1 and the decoder shown in Fig.2, Alice and Bob can complete an self-error-rejecting single-qubit transmission over a collective-noise channel with success probability $P_s = 3/4$ in a completely passive way.

For the state $[\alpha(|V\rangle_0 + |V\rangle_{\Delta t}) + \beta(|V\rangle_{\frac{\Delta t}{2}} + |V\rangle_{\frac{3\Delta t}{2}})]_{\Delta T'}$ in Eq.(4), it is not difficult to prove that Bob can perfectly obtain the uncorrupted state $|\psi\rangle = \alpha|H\rangle + \beta|V\rangle$ at the time bins $\frac{\Delta t}{2} + \Delta T'$ and $\frac{3\Delta t}{2} + \Delta T'$, which takes place with success probability 1/2, with the bit-flip operation σ_x when the single qubit emerges in port 6. On the other hand, he can also obtain the state at the time bin Δt without operations in port 6 with success probability 1/4. As the single qubit only emerges in port 6 in this state, Bob can choose the time difference between the long path and the short path in MZI$_4$ $\Delta T' = 0$ in a practical application. The similar results can be obtained for the last two terms in Eq.(4) with just a delay ΔT.

In essence, the success probability for obtaining an uncorrupted single-qubit state $|\psi\rangle = \alpha|H\rangle + \beta|V\rangle$ can be improved to be $P_s = \frac{N-1}{N}$ if an encoder can split the single qubit into $2N$ wavepackets. The wavepackets discarded by the receiver as they loss the information about the complex coefficients α and β are just the first one and the last one, shown in Fig.4. For splitting a single qubit into $2N$ wavepackets, one should only replace the MZI$_3$ in Fig.1 with the setup shown in Fig.5 in which each MZI

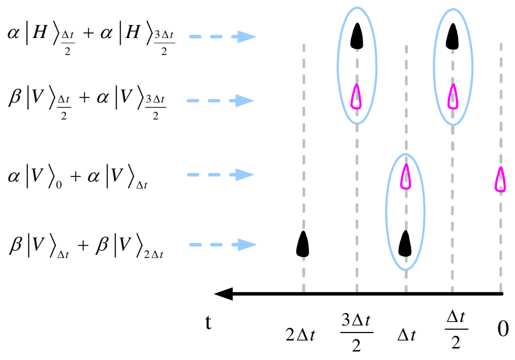
$\alpha|H\rangle_{\frac{\Delta t}{2}} + \alpha|H\rangle_{\frac{3\Delta t}{2}}$
$\beta|V\rangle_{\frac{\Delta t}{2}} + \alpha|V\rangle_{\frac{3\Delta t}{2}}$
$\alpha|V\rangle_0 + \alpha|V\rangle_{\Delta t}$
$\beta|V\rangle_{\Delta t} + \beta|V\rangle_{2\Delta t}$
t
$2\Delta t$
$\frac{3\Delta t}{2}$
Δt
$\frac{\Delta t}{2}$
0

FIG. 3: Schematic representation for the reconstruction of the original state $|\psi\rangle = \alpha|H\rangle + \beta|V\rangle$. The two wavepackets closed in an ellipse represent the fact that they will emerge in port 5 at the same time and interfere with each other, which takes place with success probability 3/4.

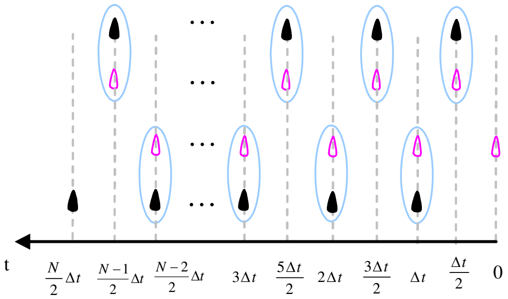

FIG. 4: Schematic representation for the reconstruction of the original state $|\psi\rangle = \alpha|H\rangle + \beta|V\rangle$ with $2N$ wavepackets. The success probability for obtaining an uncorrupted state is improved to be $\frac{N-1}{N}$.

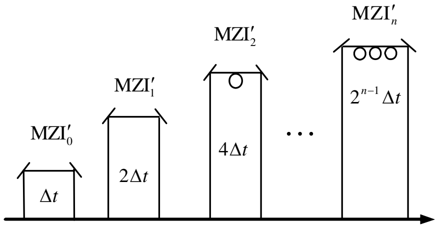

FIG. 5: A setup for splitting a single qubit into $\frac{N}{2} = 2^n$ wavepackets with unbalanced MZIs.

can be implemented in the same way as those in "plug and play" QKD systems [5, 6, 7].

We have described a passively self-error-rejecting single-qubit transmission scheme over a collective-noise channel. Compared with the novel scheme proposed by Yamamoto et al. [11] for faithful qubit distribution assisted by one additional qubit, the present scheme has some interesting features as follows: (1) The success probability for obtaining an uncorrupted state $P_S = \frac{N-1}{N}$ approaches 100% in principle if the number of wavepackets is large enough, which is about eight times of that in the scheme introduced by Yamamoto et al. [11]. At the aspect of success probability, the present scheme is an optimal one. (2) The present scheme does not require an additional qubit against a collective noise, just the single qubit itself, which makes the present scheme has some good applications in quantum communication. In detail, one can easily apply this scheme to almost all quantum communication protocols existing, such as those with single photons or entanglements [2]. Also, we can apply this scheme to the decoy-state QKD protocols [19, 20, 21] with faint laser pulses. (3) The present scheme requires only one quantum channel, not two or more [11, 12]. (4) This scheme does not require fast polarization modulators (Pockels cell) [13], i.e., it works in a completely passive way. (5) It is easy to implement this scheme with some simple optical devices in principle. (6) The success probability does not depend on the extent of the collective noise, i.e., it is independent of the noise parameters (δ_1, γ_1, δ_2, and γ_2), which is different from those in Refs.[11, 15]. As shown in Eq.(4) and Fig. 3, the wavepackets interfere with only those with the same parameter of collective noise, and the success probability for each part with the same noise parameter is $P_S = \frac{N-1}{N}$. This good feature makes the present scheme more efficient than other schemes [11, 12]. (7) As the single qubit transmitted is in an arbitrary state $|\psi\rangle = \alpha|H\rangle + \beta|V\rangle$, the present scheme can also be used to accomplish the faithful transmission of one particle in an entangled quantum system.

When the present scheme is directly applied to the decoy-state QKD protocols [19, 20, 21], the sender should send the $2N$ wavepackets to the receiver in the same signal time which is so short that the wavepackets suffer from the same noise infection. This requires the recover time of detectors is short enough. The other processes for creating a private key utilizing the present scheme with faint laser pulses is same as the decoy-state QKD protocols [19, 20, 21]. The difference is just the fact that the efficiency of detecting a photon is $\frac{N-1}{N}$ times of that in the latter.

In conclusion, we present a passively self-error-rejecting single-qubit transmission scheme for polarization states of photon, which is immune to the collective noise in quantum channel (a fiber). The success probability for obtaining an uncorrupted state, in principle, approaches 100% via postselection in different time bins with some Mach-Zehnder interferometers, independent of the parameters of collective noise, and this present scheme can be implemented with some simple optical devices and photon detectors in a completely passive way. The present scheme does not employ an entangled state in DFS, and it does not resort to additional qubits. One can directly apply this scheme to almost all quantum communication protocols against collective noise, including the decoy-state QKD protocols with faint laser pulses.

This work is supported by the National Natural Science Foundation of China under Grant No. 10604008, A Foundation for the Author of National Excellent Doctoral Dissertation of China under Grant No. 200723, and Beijing Education Committee under Grant No. XK100270454.

[1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984). p. 175.

[2] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[3] H. K. Lo and H. F. Chau, Science **283**, 2050 (1999).

[4] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[5] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, Appl. Phys. Lett. 70, 793 (1997).

[6] G. Ribordy, J. D. Gautier, N. Gisin, O. Guinnard, and H. Zbindn, Electron. Lett. 34, 2116 (1998).

[7] C. Zhou, G. Wu, X. Chen, and H. Zeng, Appl. Phys. Lett. **83**, 1692 (2003).

[8] D. A. Lidar and K. B. Whaley, arXiv: quant-ph/0301032.

[9] Z. D. Walton, A. F. Abouraddy, A. V. Sergienko, B. E. A. Saleh, and M. C. Teich, Phys. Rev. Lett. **91**, 087901 (2003).

[10] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge Univ. Press, Cambridge, 2000).

[11] T. Yamamoto, J. Shimamura, S. K. Özdemir, M. Koashi, and N. Imoto, Phys. Rev. Lett. **95**, 040503 (2005).

[12] X. H. Li, F. G. Deng, and H. Y. Zhou, Appl. Phys. Lett. **91**, 144101 (2007).

[13] D. Kalamidas, Phys. Lett. A **343**, 331 (2005).

[14] G. M. Palma, K. A. Suominen, and A. K. Ekert, Proc. R. Soc. London A **452**, 567 (1996).

[15] X. B. Wang, Phys. Rev. A **72**, 050304(R) (2005).

[16] D. B. de Brito and R. V. Ramos, Phys. Lett. A **352**, 206 (2006).

[17] J. C. Boileau, D. Gottesman, R. Laflamme, D. Poulin, and R. W. Spekkens, Phys. Rev. Lett. **92**, 017901 (2004).

[18] J. C. Boileau, R. Laflamme, M. Laforest, and C. R. Myers, Phys. Rev. Lett. **93**, 220501 (2004).

[19] W. Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).

[20] X. B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).

[21] H. K. Lo, X. F. Ma, K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).